INFORMATION ASSURANCE DIRECTORATE

"Confidence in Cyberspace"

INFORMATION ASSURANCE ADVISORY NO. IAA U/OO/802097-16

Date: 14 July 2016

SUBJECT: Recommendations to Mitigate Unauthorized Cisco® ROMMON Access and Validate Boot ROMs

DISCUSSION:

New attack methods have been observed targeting networking devices running Cisco Internetwork Operating System (IOS)® Classic platforms. Adversaries access the device with valid administrative credentials and then upload malicious code. Compromised devices are used to establish persistence and manipulate device behavior. Refer to the Cisco® Security Activity Bulletin for additional threat information. [1] This Information Assurance Advisory includes recommendations and procedures to identify the loaded ROM image and recover with a trusted ROM image, improving assurance in the device.

The ROM Monitor (ROMMON) runs during the initialization of the processor and loads the Cisco IOS® when the device is powered up or reloaded. Cisco® integrates an original read-only ROMMON image into memory during production; this image is known as the Golden ROM. Additional ROM slots, called Field Upgradable slots, are available for ROMMON upgrade images. When Cisco® provides a ROMMON upgrade, the image is loaded into a field upgradable slot. Administrators with privilege level 15 access can upload a ROMMON image from the IOS®. ROMMON upgrades can be executed either locally or remotely. If an adversary gains privileged access, the adversary will be able to upload code into the ROM of the device, thus compromising the device. The device must then be rebooted for the upgrade image to be loaded. The unauthorized ROMMON image presents an opportunity to maintain persistence after reboot without altering the boot IOS®; thus increasing the difficulty to detect its presence. A combination of network hygiene and security policy can detect indications and mitigate unauthorized ROMMON access. IAD recommends the following to mitigate unauthorized ROMMON access:

- Protect Administrator Credentials from Unauthorized Access to Networking Devices
- Monitor Device Logs to Identify Unauthorized Device Modification
- Validate and Restore with a Trusted ROMMON Image

Protect Administrator Credentials from Unauthorized Access to Networking Devices

- Implement a configuration management plan with security policies to administer system upgrades and configurations.
- Strengthen physical security and enforce security policies.
- Implement hard tokens, specifically, time-based synchronized authentication, to provide protection against unauthorized access to administrator accounts.
- Implement Cisco® recommended best practices to supplement security efforts to restrict privileged access to network devices:

  - Cisco® Guide to Harden Cisco IOS® Devices [2]
  - Cisco IOS® Software Integrity Assurance [3]
  - Cisco IOS® Image Verification [4]

- Follow Defense Information Systems Agency Security Technical Implementation Guides [5] (DISA STIGs). IAD recommends the following DISA STIGs to securely install and maintain DoD devices and systems (STIG Rule ID):
  - The network element must be password protected (SV-3012r2_rule).
  - Group accounts must not be configured for use on the network device (SV-3056r5_rule).
  - Management connections to a network device must be established using secure protocols with FIPS 140-2 validated cryptographic modules (SV-15451r3_rule).
  - The network element must not have any default manufacturer passwords (SV-3143r2_rule).
  - The network device must require authentication for console access (SV-19270r3_rule).
  - The network devices must require authentication prior to establishing a management connection for administrative access (SV-16259r2_rule).
  - Authorized accounts must be assigned the least privilege level necessary to perform assigned duties. (SV-15471r3_rule).

Monitor Device Logs to Identify Unauthorized Device Modification

- Monitor system and device logs for evidence of unauthorized access and system changes.
- Monitor administrative information like system upgrades, management connections, and boot history. Information discrepancies and unauthorized actions should be identified. Log data should be written and protected on a remote server.
- Follow DISA STIGs. IAD recommends the following DISA STIGs to securely monitor DoD devices and systems (STIG RuleID):
  - The network element must log all messages except debugging and send all log data to a syslog server (SV-15476r2_rule).
  - The network element must log all attempts to establish a management connection for administrative access (SV-15455r2_rule).
  - The network element must only allow management connections for administrative access from hosts residing into the management network (SV-15449r2_rule).

Validate and Restore with a Trusted ROMMON Image

Cisco® manufactures networking devices with multiple ROM slots designed for the integrated read-only Golden ROM image and the field upgradable ROMs.

Devices will boot from the Golden ROM image by default and have the option of booting from the field upgradable ROM. If the device is booting from the Golden ROM, it does not need to be changed. If the device is booting off the field upgradable ROM, it could be at risk of using an unauthorized ROMMON image and must be reloaded with a trusted upgrade image. The following procedure will determine whether the device is at risk.

- Identify which ROM the device boots from using the Cisco IOS® commands:
  - show rom-monitor
  - show version

Devices which boot from the Field Upgradable ROM are subject to further inspection. To restore the device with a trusted image, overwrite the field upgradable ROM with a trusted upgrade image from a trusted source. The following procedure outlines steps using Cisco IOS® CLI to restore the device with a trusted image.

- Establish a ROMMON image baseline:
    - show rom-monitor
    - show version

- Set the device to boot from the Golden ROM image:
    - upgrade rom-monitor preference readonly
    - reload

- Upload a trusted ROMMON upgrade image. This process will overwrite the image stored in the Field Upgradable ROM slot:
    - upgrade rom-monitor file <location>
    - This command will result in a 'power-on reset' of the router! Continue? [yes/no] yes

- Set the preference boot image to the new upgrade image:
    - upgrade rom-monitor preference upgrade
    - reload

- Document the ROMMON image and validate the state of the device:
    - show rom-monitor
    - show version

- When reloading to a trusted ROM, always use newly created trusted credentials.

    Network administrators should always consider replacing antiquated devices with ones incorporating Trust Anchor Module, Secure Boot, and signed image capabilities. These capabilities validate firmware authenticity and integrity; thus, increasing the confidence of an unmodified platform [6]. Always purchase network hardware from authorized resellers certified by Cisco® to minimize the risk of supply chain tampering.

References:
[1] tools.cisco.com/security/center/viewAlert.x?alertId=40411
[2] www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html
[3] www.cisco.com/web/about/security/intelligence/integrity-assurance.html
[4] www.cisco.com/web/about/security/intelligence/iosimage.html
[5] iase.disa.mil/stigs/Pages/index.aspx
[6] www.cisco.com/web/about/doing_business/trust-center/docs/trust-anchor-technologies-ds-45-734230.pdf

Cisco® is a registered trademark of Cisco Systems, Inc.
Cisco IOS® is a registered trademark of Cisco Systems, Inc.

Disclaimer of Endorsement:
The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

For further information about this product, please contact:

Industry Inquiries
410-854-6091
email: bao@nsa.gov

Client Requirements And General Information Assurance Inquiries
IAD Client Contact Center
410-854-4200
email: IAD_CCC@nsa.gov